ABSTRACT

An optical disk is provided that disables reproduction of sub-information even if the sub-information as a contents encryption key is recorded entirely onto another optical disk. Sub-information is recorded on the optical disk by deforming a recording mark slightly in accordance with a pseudo random number sequence that is obtained using as an initial value medium ID that is read out medium inherent information. This allows sub-information inherent in a medium to be recorded, and even if the sub-information is duplicated entirely to another optical disk, the illegally duplicated sub-information cannot be reproduced because of a difference in initial value of a pseudo random number sequence between media.